PATENT COOPERATION TREATY

PCT

RECD 28 DEC 2004
WIPO PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Rec'd PCT/PTO 15 APR 2005

Applicant's or agent's file reference 6/NP/W40013WO	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/GB 03/04371	International filing date *(day/month/year)* 09.10.2003	Priority date *(day/month/year)* 17.10.2002
International Patent Classification (IPC) or both national classification and IPC G06F17/60		
Applicant VODAFONE GROUP PLC.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 9 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the opinion
   - II ☐ Priority
   - III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
14.05.2004	28.12.2004
Name and mailing address of the international preliminary examining authority: European Patent Office - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Authorized Officer Rüster, H-B Telephone No. +31 70 340-2644

BEST AVAILABLE COPY

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB 03/04371

I. Basis of the report

1. With regard to the **elements** of the international application *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17))*:

Description, Pages

1-6, 8-45	as originally filed
7	received on 20.09.2004 with letter of 20.09.2004

Claims, Numbers

1-51	received on 20.09.2004 with letter of 20.09.2004

Drawings, Sheets

1-13	as originally filed

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

   These elements were available or furnished to this Authority in the following language: , which is:

   ☐ the language of a translation furnished for the purposes of the international search (under Rule 23.1(b)).

   ☐ the language of publication of the international application (under Rule 48.3(b)).

   ☐ the language of a translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

   ☐ contained in the international application in written form.

   ☐ filed together with the international application in computer readable form.

   ☐ furnished subsequently to this Authority in written form.

   ☐ furnished subsequently to this Authority in computer readable form.

   ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

   ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. The amendments have resulted in the cancellation of:

   ☐ the description, pages:

   ☐ the claims, Nos.:

   ☐ the drawings, sheets:

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)).

   (Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.)

6. Additional observations, if necessary:

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-51
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-51
Industrial applicability (IA)	Yes:	Claims	1-51
	No:	Claims	

2. Citations and explanations

see separate sheet

1. The amendment of new claims 1, 21 and 42 go beyond the disclosure in the international application as filed (Article 34(2)(b) PCT), because the term "telecommunications terminal" cannot be found in nor unambiguously derived from the original application.

2. Current claim 1 obviously claims protection for the use of a generally well known SIM based authentication process of a cellular for further authentication processes outside of a standard telecommunication system.

   The skilled person, familiar with telecommunication authentication standards would not even need a document to apply this standard in a different data processing environment to come to the solution taught by claim 1. Thus, the subject matter of claim 1 does not comprise an inventive step (Article 33 (3) PCT).

3. Referring to the amended claims, the following, not yet cited Document D2 is introduced (Rule 64.1 PCT).

   D2: EP-A-0 727 894 (KOKUSAI DENSHIN DENWA CO. LTD; TOKYO (JP)) 21 August 1996 (1996-08-21)

4. Document D2 is now besides document D1 considered to represent the closest state of the art (comments in brackets relate to D2).

   Compared to claim 1, document D2 (see claim 3; figs. 1 and 2 and related description) discloses a device (card reader 11) for connection to a data processing apparatus (client terminal 12), the device (card reader 11) including authentication storage means (smart card 10) operatively coupled thereto for storing predetermined authentication information respective to a user (AuInf), the authentication storage means (smart card 10) being registered with a telecommunications system (authentication center) which includes authenticating means (AuC data), the device (card reader 11), when operatively coupled to the authentication storage means (smart card 10), being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means (AuC data) to carry out the authentication process via a communication link (network 13) with the authenticating means (AuC data) in the said telecommunications system (authentication center) whereby to authenticate a subsequent transaction by the user with the dataprocessing apparatus (client terminal 12), and which involves

use of the data carried by the authentication storage means (smart card 10), the predetermined authentication information stored by the authentication storage means (smart card 10) corresponding to information which is used to authenticate the user registered with the telecommunications system (authentication center) in relation to use of that users telecommunications terminal in the telecommunications system (authentication center).

The remaing difference between subject matters of claim 1 and the device of document D2 is the (not originally disclosed) "telecommunications terminal" also useable by the authentication means.

The objective problem would be to introduce multiply useable authentication means in the device known by document D2.

The skilled person, confronted with this problem would have resolved it by the means of claim 1 without inventive activity, as it is common knowledge to swap and use authentication storage means, such as (cellular) SIM cards between communication devices.

Thus, the subject-matter of claim 1 does not meet the requirements of Article 33(1) PCT as not involving an inventive step in the sense of Article 33(3) PCT.

5. Independent claim 21 (method) is based on the same combination of features of claim 1, adapted to the category of claim, and independent claim 42 (device) differs from claim 1 only in that the authentication storage means are included rather than connected to a device.
Consequently, the assessment made for claim 1 is equivalently valid also here: The subject-matter of claims 21 and 42 does not meet the requirements of Article 33(1) PCT as not involving an inventive step in the sense of Article 33(3) PCT.

6. The dependent claims comprise additional features which are either rendered obvious by, or explicitly known from D2 for the skilled person.
In this context the subject-matter of claims 2-20, 22-41 and 43-51 do not meet the requirements of Article 33(1) PCT as not involving an inventive step in the sense of Article 33(3) PCT.

Burkhart Rüster

ART 34 AMDT

authentication process can be carried out. In a case where the SIM is the SIM of a subscriber to a particular cellular telecommunications network, the authentication process can be carried out by that network.

It should be noted that the authentication process being described does not necessarily authenticate the human identity of the user. For example, cellular telecommunication networks have pre-pay subscribers who are issued with SIMs in return for pre-payment enabling them to make calls on the network. However, the identity of such pre-pay subscribers is not known (or not necessarily known) by the networks. Nevertheless, such a user cannot make use of the network until the network has authenticated that user's SIM – that is, has confirmed that such user is a particular user who has a particular pre-paid account with the network. The SIMs of such pre-paid users or subscribers could equally well be used (in the manner described) in or in association with data processing apparatus or computers, for the purposes of authenticating that user.

The SIM need not take the form of a physical (and removable) smart card but instead can be simulated by being embedded in the data processing apparatus or computer in the form of software or represented as a chip for example.

It may be desirable to be able to change the authentication information on the SIM (or simulated SIM) to take account of changed circumstances. For example, the SIM may be a SIM registered with a particular cellular telecommunications network – a network applicable to the country or region where the data processing apparatus or computer is to be used. However, circumstances may arise (for example, the apparatus or the computer is physically moved to a different country or region) in which it is desirable or necessary to re-register the SIM with a different cellular telecommunications network. Ways in which this can be done are disclosed in our co-pending United Kingdom patent publications Nos. 2378094, 2378096 and 2378097 and in our corresponding PCT publications Nos. WO03/013174,WO03/013173 and WO03/013172. As described therein

ART 34 AMDT

CLAIMS

1. A device (30) for connection to a data processing apparatus (10), the device including authentication storage means (12) operatively coupled thereto for storing predetermined authentication information respective to a user, the authentication storage means (12) being registered with a telecommunications system (16) which includes authenticating means (18;102) and for which the user has a telecommunications terminal, the device, when operatively coupled to the authentication storage means (12), being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means (18;102) to carry out the authentication process via a communication link (19) with the authenticating means (18;102) in the said telecommunications system (16) whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means (12), the predetermined authentication information stored by the authentication storage means (12) corresponding to information which is used to authenticate the user registered with the telecommunications system (16) in relation to use of that user's telecommunications terminal in the telecommunications system (16).

2. The device of claim 1, comprising security data entry means (46) for obtaining security data independently of the data processing apparatus (10), and means for analysing the entered security data for determining whether to allow access to the predetermined information.

3. The device of claim 2, wherein the security data entry means (46) comprises alphanumeric data entry means.

4. The device of claim 2 or 3, wherein the security data entry means (46) comprises a

ART 34 AMDT

keypad.

5. The device of claim 2,3 or 4, wherein the security data comprises a Personal Identification Number (PIN) and the analysing means compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means and only allows access to the predetermined information when the respective PINs match.

6. The device of any one of the preceding claims, comprising a display (48) for displaying security information.

7. The device of any one of the preceding claims, comprising a data processing module (36) for controlling the communication with the data processing apparatus (10).

8. The device of claim 7, wherein the data processing module (36) of the device (30) is configured for communicating with a corresponding data processing module (38) of the data processing apparatus (10).

9. The device of claim 8, wherein communication between the authentication storage means (12) and the data processing apparatus (10) is performed via the respective data processing modules (36,38).

10. The device of claim 7,8 or 9, wherein the data processing module (36) of the device (30) includes means for decrypting encrypted data received from the data processing module (38) of the data processing apparatus (10).

11. The device of claim 7,8,9 or 10, wherein the data processing module (36) of the device (30) includes means for encrypting data transmitted to the data processing module (38) of the data processing apparatus (10).

ART 34 AMDT

12. The device of claims 10 or 11, wherein the respective data processing modules (36,38) comprise a key for allowing encryption and/or decryption of data.

13. The device of claim 12, wherein the key comprises a shared secret key for each of the respective data processing modules (36,38).

14. The device of any one of claims 1 to 13, in which each user is authenticated in the telecommunications system by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means (12) respective to that user corresponds to or simulates the smart card for that user.

15. The device of any one of claims 1 to 14, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

16. The device of any one of claims 1 to 15, in which the authentication storage means (12) is specific to that device (30).

17. The device of any one of claims 1 to 16, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

18. The device of any one of claims 14 to 17, wherein the telecommunications system (16) includes means for levying a charge for the transaction when authorised.

19. The device of any one of the preceding claims in combination with the data processing apparatus (10).

20. The device of any one of the preceding claims in combination with the telecommunications system (16).

ART 34 AMDT

21. A method for authenticating a transaction with data processing apparatus (10) in which the data processing apparatus (10) has operatively associated with it a security device (30) which in turn has operatively associated with it authentication storage means (12) for storing predetermined authentication information respective to a user, the authentication storage means (12) being registered with a telecommunications system (16) which includes authenticating means (18;102) and for which the user has a telecommunications terminal, the device, when operatively coupled to the authentication storage means (12), being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means. (18;102) to carry out the authentication process via a communication link (19) with the authenticating means (18;102) in the said telecommunications system (16) whereby to authenticate a subsequent transaction by the user with the data processing apparatus and which involves use of the data carried by the authentication storage means (12), the predetermined authentication information stored by the authentication storage means (12) corresponding to information which is used to authenticate the user registered with the telecommunications system (16) in relation to use of that user's telecommunications terminal in the telecommunications system (16), the predetermined authentication information being obtained from the authentication storage means (12) via the security device (30) which controls access to the predetermined authentication information.

22. The method of claim 21, comprising obtaining security data independently of the data processing apparatus (10), and analysing the security data for determining whether to allow access to the predetermined information.

23. The method of claim 22, wherein the security data is obtained by alphanumeric data entry means (46).

ART 34 AMDT

24. The method of claim 21 or 23, wherein the alphanumeric data entry means (46) comprises a keypad.

25. The method of claim 22,23 or 24, wherein the security data comprises a Personal Identification Number (PIN) and the analysing step compares the PIN obtained by the security data entry means with a PIN stored on the authentication storage means (12) and only allows access to the predetermined information when the respective PINs match.

26. The method of any one of claims 21 to 25, comprising displaying security information.

27. The method of any one of claims 21 to 26, wherein communication with the data processing apparatus is controlled by a data processing module (36).

28. The method of claim 27, wherein the data processing module (36) of the device (30) is configured for communicating with a corresponding data processing module (38) of the data processing apparatus (10).

29. The method of claim 28, wherein communication between the authentication storage means (12) and the data processing apparatus (10) is performed via the respective data processing modules (36,38).

30. The method of claim 27,28 or 29, wherein the data processing module (36) of the device (30) decrypts encrypted data received from the data processing module (38) of the data processing apparatus (10).

31. The method of claim 27,28,29 or 30, wherein the data processing module (36) of the device (30) encrypts data transmitted to the data processing module (38) of the data processing apparatus (10).

ART 34 AMDT

32. The method of claims 30 and 31, wherein the respective data processing modules 36,38 comprise a key for allowing encryption and/or decryption of data.

33. The method of claim 32, wherein the key comprises a shared secret key for each of the respective data processing modules (36,38).

34. A method according to any one of claims 21 to 33, in which each user is authenticated in the telecommunications system (16) by means of the use of a smart card or subscriber identity module (e.g. SIM), and in which the authentication storage means respective to that user corresponds to or simulates the smart card for that user.

35. A method according to any one of claims 21 to 34, in which the transaction is a transaction involving use of the data processing functions of the data processing apparatus.

36. A method according to any one of claims 21 to 35, in which each authentication storage means (12) is associated with a specific security device (30).

37. A method according to any one of claims 21 to 36, in which the authentication storage means (12) is associated with the data processing apparatus (10) by being associated with data or software for use by that data processing apparatus 10).

38. A method according to any one of claims 21 to 39, in which the authentication process involves the sending of a message and the generation of a response dependent on the message and the predetermined information.

39. A method according to any one of claims 21 to 40, including the step of levying a charge for the transaction when authenticated.

ART 34 AMDT

40. A method according to claim 39, in which the step of levying the charge is carried out by the said telecommunication system (16).

41. A method according to any one of claims 21 to 40, in which the data processing apparatus (10) is a personal computer.

42. A device including authentication storage means (12) for controlling access to predetermined authentication information stored on the authentication storage means (12), the device including means for coupling the device to a data processing apparatus (10) to allow the authentication information to be used to authenticate a transaction performed by the data processing apparatus (10), the predetermined authentication information stored on the authentication storage means (12) being respective to a user, the authentication storage means (12) being registered with a telecommunications system (16) which includes authenticating means (18;102) and for which the user has a telecommunications terminal, the device, when operatively coupled to the authentication storage means (12), being responsive to an input message for deriving a response dependent on the input message and on the authentication information for enabling the authenticating means (18;102) to carry out the authentication process via a communication link (19) with the authenticating means (18;102) in the said telecommunications system (16) whereby to authenticate the transaction by the user with the data processing apparatus, and wherein security means is provided for controlling access to the authentication information via the data processing apparatus.

43. The device of claim 42, wherein the security means comprises means (46) for obtaining security data from a user and means for checking the validity of the security data and only allowing access to the authentication data if the security data is valid.

44. The device of claim 42 or 43, wherein the security means comprises data

ART 34 AMDT

processing means (36) for receiving an encrypted authentication request, encrypted using a predetermined key, from the data processing apparatus (10) and for decrypting the request.

45. The device of claim 44 in combination with the data processing apparatus (10), wherein the data processing apparatus (10) comprises means for encrypting the authentication request using said key.

46. A device according to any one of claims 1 to 20 or 42 to 45, wherein the device (30) communicates wirelessly to authenticate the transaction.

47. A device according to claim 14, wherein the smart card or SIM authenticates the transaction when the smart card or SIM is operable in a mobile terminal.

48. A device according to claim 14, wherein the smart card or SIM is further operable to authenticate a mobile terminal for use in the system.

49. A method according to any one of claims 21 to 41, wherein the security device (30) communicates wirelessly to authenticate the transaction.

50. A method according to claim 34, wherein the smart card or SIM authenticates the transaction when the smart card or SIM is operable in a mobile terminal.

51. A method according to claim 34, wherein the smart card or SIM is further operable to authenticate a mobile terminal for use in the system.

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☑ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☑ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.